Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • CCST Cybersecurity

Cisco Certified Support Technician – Cybersecurity

Formation d'initiation à la cybersécurité centrée sur les principes essentiels, la sécurité réseau, la protection des postes de travail, la gestion des vulnérabilités et la réponse aux incidents, pour préparer et réussir l'examen Cisco Certified Support Technician – Cybersecurity.

Durée	Examen
23 h (recommandé)	CCST Cybersecurity
Modalité	**Niveau**
Distanciel	Fondamental / Entry-level

Distributeur officiel Certiport | Centre d'examen Certiport | Learn • Practice • Certify

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

- **Learn** : Compréhension des principes clés de la cybersécurité, des menaces, de l'architecture réseau et des mesures de protection.
- **Practice** : Pratique sur cas concrets avec outils de sécurité de base, conforme aux objectifs de l'examen CCST Cybersecurity.
- **Certify** : Passage de l'examen Cisco Certified Support Technician – Cybersecurity avec voucher optionnel.

OBJECTIFS PÉDAGOGIQUES

- La formation couvre les principes de cybersécurité, les menaces majeures et les réflexes de protection.
- Elle inclut la sécurité réseau, les technologies d'accès sécurisé et la protection des postes de travail.
- Elle aborde également la gestion des vulnérabilités, l'analyse de risques et le traitement des incidents.

PUBLIC CIBLE

- La formation s'adresse aux débutants et professionnels IT souhaitant acquérir une base en cybersécurité et une première certification Cisco.
- Elle concerne également toute personne impliquée dans la protection des systèmes d'information.

PRÉREQUIS

- Connaissances générales en informatique et en réseaux (niveau débutant).
- Intérêt pour la cybersécurité et la protection des systèmes d'information.

© 2026 Smartfuture — Cisco Certified Support Technician – Cybersecurity

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Principes essentiels de sécurité (Essential Security Principles)

Définir les principes essentiels de sécurité

- Vulnérabilités, menaces, exploits et risques ; vecteurs d'attaque ; hardening ; défense en profondeur (defense-in-depth) ; confidentialité, intégrité et disponibilité (CIA) ; types d'attaquants ; motivations des attaques ; code d'éthique.

Expliquer les menaces et vulnérabilités courantes

- Malware, ransomware, déni de service (DoS), botnets, attaques d'ingénierie sociale (tailgating, spear phishing, phishing, vishing, smishing, etc.), attaques physiques, man-in-the-middle, vulnérabilités IoT, menaces internes (insider threats), menaces persistantes avancées (APT).

Expliquer les principes de gestion des accès

- Authentication, authorization et accounting (AAA) ; RADIUS ; authentification multifactorielle (MFA) ; politiques de mots de passe.

Expliquer les méthodes de chiffrement et leurs applications

- Types de chiffrement, fonctions de hachage (hashing), certificats, infrastructure à clés publiques (PKI) ; algorithmes forts vs faibles ; états des données et chiffrement approprié (données en transit, au repos, en cours d'utilisation) ; protocoles utilisant le chiffrement.

Concepts de base de la sécurité réseau (Basic Network Security Concepts)

Décrire les vulnérabilités des protocoles TCP/IP

- Vulnérabilités associées aux protocoles TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS et leur exploitation potentielle.

© 2026 Smartfuture — Cisco Certified Support Technician – Cybersecurity

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Expliquer l'impact des adresses réseau sur la sécurité

- Adresses IPv4 et IPv6, adresses MAC, segmentation réseau, notation CIDR, NAT, différence entre réseaux publics et privés.

Décrire l'infrastructure réseau et les technologies associées

- Architecture de sécurité réseau, DMZ, virtualisation, cloud, honeypot, serveur proxy, systèmes de détection et de prévention d'intrusion (IDS/IPS).

Configurer un réseau sans fil SoHo sécurisé

- Filtrage d'adresses MAC, standards et protocoles de chiffrement Wi-Fi, paramètres SSID et bonnes pratiques de sécurisation d'un routeur domestique/pro.

Mettre en œuvre des technologies d'accès sécurisé

- Listes de contrôle d'accès (ACL), pare-feu, VPN, Network Access Control (NAC) et principes d'implémentation.

Concepts de sécurité des endpoints (Endpoint Security Concepts)

Décrire les concepts de sécurité des systèmes d'exploitation

- Sécurité sur Windows, macOS et Linux ; fonctionnalités de sécurité (Windows Defender, pare-feux locaux, etc.) ; utilisation de la ligne de commande et de PowerShell ; droits d'accès aux fichiers et répertoires ; escalade de privilèges.

Utiliser les outils appropriés de sécurité des endpoints

- Familiarisation avec des outils tels que netstat, nslookup, tcpdump pour collecter des informations de sécurité et diagnostiquer les communications réseau.

Vérifier la conformité des endpoints aux politiques de sécurité

- Gestion des inventaires matériels et logiciels (asset management), déploiement de programmes, sauvegarde des données, conformité réglementaire (PCI DSS, HIPAA, GDPR), gestion des appareils personnels (BYOD), chiffrement des données, distribution d'applications et gestion de la configuration.

Mettre en œuvre les mises à jour logicielles et matérielles

- Windows Update, mises à jour applicatives, pilotes de périphériques, firmware, stratégies de patch management.

© 2026 Smartfuture — Cisco Certified Support Technician – Cybersecurity

Interpréter les journaux système

- Utilisation de l'Observateur d'événements (Event Viewer), journaux d'audit, journaux système et applicatifs, syslog, identification des anomalies dans les logs.

Connaître les principes de base de la suppression de malware

- Analyse des systèmes, examen des journaux d'analyse, processus de remédiation après détection de malware.

Analyse de vulnérabilités et gestion des risques (Vulnerability Assessment and Risk Management)

Expliquer la gestion des vulnérabilités

- Identification, gestion et atténuation des vulnérabilités ; reconnaissance active et passive ; tests (scan de ports, automatisation des analyses).

Utiliser le renseignement sur les menaces (threat intelligence)

- Utilisation et limites des bases de vulnérabilités ; outils standards pour évaluer les vulnérabilités et formuler des recommandations, politiques et rapports ; Common Vulnerabilities and Exposures (CVEs), rapports de cybersécurité, actualités, services d'abonnement et intelligence collective ; renseignement ad hoc et automatisé ; importance de la mise à jour de la documentation et de la communication avant, pendant et après les incidents ; sécurisation, partage et mise à jour de la documentation.

Expliquer la gestion des risques

- Différence entre vulnérabilité et risque, hiérarchisation des risques, approches de gestion, stratégies d'atténuation, niveaux de risque (faible, moyen, élevé, extrêmement élevé), risques liés aux types de données et à leur classification, évaluations de sécurité des systèmes informatiques (sécurité de l'information, gestion des changements, opérations informatiques, assurance de l'information).

© 2026 Smartfuture — Cisco Certified Support Technician – Cybersecurity

Expliquer l'importance du plan de reprise après sinistre et de continuité d'activité

- Catégories de sinistres (naturels et d'origine humaine), caractéristiques des plans de reprise d'activité (DRP) et de continuité d'activité (BCP), sauvegardes, contrôles de reprise après sinistre (détectifs, préventifs et correctifs).

Gestion des incidents (Incident Handling)

Surveiller les événements de sécurité et savoir quand escalader

- Rôle des solutions SIEM et SOAR ; surveillance des données réseau pour identifier les incidents (captures de paquets, entrées de journaux, etc.) ; identification d'événements suspects en temps réel.

Expliquer la recherche de preuves numériques et l'attribution des attaques

- Cyber Kill Chain, matrice MITRE ATT&CK, Diamond Model ; tactiques, techniques et procédures (TTP) ; sources de preuves (artifacts) ; gestion des preuves (préservation, chaîne de conservation/chain of custody).

Expliquer l'impact des cadres de conformité sur la gestion des incidents

- Cadres de conformité (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), exigences en matière de rapports et de notifications après incidents.

Décrire les éléments de la réponse aux incidents de cybersécurité

- Politiques, plans et procédures de réponse aux incidents ; étapes du cycle de vie de la réponse aux incidents selon le NIST SP 800-61 (préparation, détection et analyse, confinement, éradication, récupération, retour d'expérience).

© 2026 Smartfuture — Cisco Certified Support Technician – Cybersecurity